

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of

FCC Review of Regulatory Requirements
for IP-Enabled Services

WC Docket No. 04-36

TO: The Commission

**COMMENTS OF THE
DEPARTMENT OF HOMELAND SECURITY**

TABLE OF CONTENTS

TABLE OF CONTENTS.....	ii
I. INTRODUCTION AND SUMMARY.....	1
II. BACKGROUND OF THE FCC’S PROPOSED RULE.....	4
III. STATEMENT OF INTEREST AND POSITION.....	5
A. INFRASTRUCTURE PROTECTION.....	5
1. BACKGROUND ON NCS.....	5
2. STATEMENT OF INTEREST AND POSITION.....	6
(a) STATEMENT OF INTEREST.....	6
(b) STATEMENT OF POSITION.....	10
B. LAW ENFORCEMENT, NATIONAL SECURITY, AND PUBLIC SAFETY.....	11
1. BACKGROUND.....	11
2. STATEMENT OF INTEREST AND POSITION.....	11
(a) STATEMENT OF INTEREST.....	11
(i) USSS.....	11
(ii) ICE.....	12
(iii) USCG.....	14
(b) STATEMENT OF POSITION.....	14
IV. CONCLUSION.....	16

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of)	
)	
)	
FCC Review of Regulatory Requirements)	WC Docket No. 04-36
for IP-Enabled Services)	
)	
_____)	

TO: The Commission

**COMMENTS OF THE
DEPARTMENT OF HOMELAND SECURITY**

The UNITED STATES DEPARTMENT OF HOMELAND SECURITY (“DHS” or “the Department”), pursuant to Section 1.415 of the rules of the Federal Communications Commission (“FCC” or “Commission”), 47 C.F.R. § 1.415 (2003), hereby submits these Comments in response to the Commission’s Notice of Proposed Rule Making in the proceeding captioned above (“the FCC’s Proposed Rule”).¹ These comments address two sets of DHS equities: (1) the critical infrastructure protection responsibilities of DHS’s Information Analysis and Infrastructure Protection (“IAIP”) Directorate, including the functions of DHS in leading the National Communication System (“NCS”); and (2) the law enforcement, national security, and public safety equities of DHS’s Border and Transportation Security (“BTS”) Directorate, including the functions of United States Immigration and Customs Enforcement (“ICE”), and the United States Secret Service (“USSS”) and United States Coast Guard (“USCG”).

I. INTRODUCTION AND SUMMARY

By law, all functions of “officers, employees, and organizational units” within the

¹ Review of Regulatory Requirements for IP-Enabled Services, 69 FR 16193, Monday, March 29, 2004.

Department of Homeland Security (“DHS”) are vested in the Secretary.² As part of its statutory mission,³ DHS has been tasked to carry out the missions and functions of elements transferred into the Department. One of the federal activities transferred into the Department was the NCS functions of the Department of Defense.⁴ These infrastructure protection functions form one set of equities DHS is addressing in some detail in these comments on FCC’s Proposed Rule.

In summary, with respect to the Department’s infrastructure protection responsibilities, DHS believes that in the evolving IP-enabled environment both legacy voice telecommunications services and newly introduced information services must be utilized to meet NCS National Security and Emergency Preparedness (“NS/EP”) telecommunications requirements.⁵ While DHS/NCS is pursuing voluntary arrangements, these NS/EP services may require exceptional government regulatory consideration to ensure the NS/EP users receive the priority treatment they need to fulfill their missions during national emergencies. NS/EP considerations provide a compelling rationale for the FCC to abstain from closing the door to addressing these issues by regulation of IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services to Federal, state and local government officials and first responders in times of emergency or national crisis. The NCS strongly encourages the FCC to include existing NS/EP considerations in the forefront of their deliberations regarding IP-enabled services and protect the ability of the FCC to regulate these services for this purpose should that become necessary in the future. Finally, as part of the current Proposed Rulemaking, the Commission is respectfully requested to consider incorporating guidance on national security requirements for both the telecommunications

² See The Homeland Security Act of 2002, Public Law 107–296, November 25, 2002, § 102(a)(3), 6 U.S.C. § 112(a)(3).

³ P.L. 107-296, § 101(b)(1)(D), 6 U.S.C. § 111(b).

⁴ P.L. 107-296, § 201(g)(2), 6 U.S.C. § 121(g)(2).

⁵ Report of the White House Convergence Task Force, December 29, 2000.

infrastructure and all elements of the information technology infrastructure subject to its jurisdiction. These points are discussed in detail below. In addition, DHS stands ready to assist the Commission further in this respect.

Apart from infrastructure protection concerns, in addition, several agencies with law enforcement, national security, and public safety missions and functions were also transferred into DHS, including the United States Secret Service, the United States Customs Service, and the United States Coast Guard.⁶ Those missions and functions form a second set of equities DHS is addressing in these comments on the FCC's Proposed Rule. However, with respect to those missions and functions, DHS has already coordinated extensively with the Justice Department ("DOJ") and notes that the DOJ (with the Federal Bureau of Investigation and the Drug Enforcement Administration) has already filed a Joint Petition for Rulemaking with the Commission that asks the Commission to determine which services, including IP-enabled services, and entities, are subject to the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001-1021.⁷ DHS concurs with that Joint Petition and notes that many of the subjects and questions raised by the Commission in the FCC's Proposed Rule have the potential to impact CALEA implementation under the Joint Petition. The DOJ is submitting comments in this docket concerning the potential impact on CALEA of the Commission's regulatory treatment of IP-enabled services in the FCC's Proposed Rule, as well as law enforcement and national security concerns regarding access to sensitive network information

⁶ P.L. 107-296, §§ 801, 403, and 888 (respectively), 6 U.S.C. §§ 381, 203, and 468 (respectively); subsequently, the Customs criminal enforcement functions were subsumed in the DHS Bureau of Customs and Immigration Enforcement ("ICE"), pursuant to the President's Reorganization Plan of November 25, 2002, as amended by the President's January 30, 2003, modification.

⁷ *In the Matter of United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act*, RM No. 10865 (filed Mar. 10, 2004) (hereinafter "CALEA Joint Petition").

and international communications service authorizations for such services.⁸ DHS joins in those DOJ comments and thus it is only necessary below to provide background on DHS's equities to assist the Commission in its deliberations.

II. BACKGROUND OF THE FCC'S PROPOSED RULE

The FCC initiated the FCC's Proposed Rule in order to "examine issues relating to the services and applications making use of IP, including but not limited to voice over IP ("VoIP") services (collectively, "IP-Enabled services").⁹ The FCC defines "IP-enabled services" to include "services and applications relying on the Internet protocol family" which includes software that can be used by customers to communicate.¹⁰

Two of the FCC's goals in the FCC's Proposed Rule are to: (1) identify those IP-enabled services that are available today and those expected to be available in the future; and (2) to determine whether any regulatory treatment is appropriate for any class of IP-enabled services.¹¹ The FCC explicitly states that its "aim in this proceeding is to facilitate this transition [to IP-enabled services], relying wherever possible on competition and applying discrete regulatory requirements only where such requirements are necessary to fulfill important policy objectives."¹² The FCC stated that "other aspects of the existing regulatory framework -- including those provisions designed to ensure disability access, consumer protection, emergency 911 service, law enforcement access for authorized wiretapping purposes, consumer privacy, and

⁸ As the Commission recognized in the FCC's Proposed Rule, "[t]his Notice does not prejudice the outcome of our proceeding on CALEA, and we will closely coordinate our efforts in these two dockets." FCC's Proposed Rule at ¶ 50 n.158.

⁹ FCC's Proposed Rule at ¶ 1.

¹⁰ *Id.* An example of such an "application" is pulver.com's Free World Dialup service that the FCC recently held was not a telecommunications service because it does not include any transmission component. *In re Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, WC Docket No. 03-45, FCC 04-27, at ¶ 8 (rel. February 19, 2004).

¹¹ FCC's Proposed Rule at ¶ 2.

¹² *Id.* at ¶ 5.

others -- should continue to have relevance as communications migrate to IP-enabled services."¹³

However, the FCC refused to conclude in the FCC's Proposed Rule that such so-called social policies should apply to IP-enabled services and sought comment on these matters in the FCC's Proposed Rule.¹⁴

III. STATEMENT OF INTEREST AND POSITION

A. Infrastructure Protection

1. Background on NCS

As noted above, the Homeland Security Act of 2002 transferred the functions, personnel, assets and liabilities of the NCS to the Secretary of DHS.¹⁵ The NCS itself consists of the telecommunications assets of the 23 major Federal Departments and Agencies represented on the NCS Committee of Principals. The Secretary of Homeland Security is assigned the additional duty of Executive Agent of the NCS under the authority of Executive Order (EO) Number 12472¹⁶, as amended by EO 13286¹⁷. The NCS is responsible for "the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution." Further, EO 12472 directs that: "The NCS shall seek to ensure that a national telecommunications infrastructure is developed which:

(1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government;

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *See*, footnote 4, *supra*.

¹⁶ Assignment of National Security and Emergency Preparedness Telecommunications Functions", April 3, 1984

¹⁷ Amendment of Executive Orders and Other Actions In Connection With the Transfer of Certain Functions to the Secretary of Homeland Security", February 28, 2003

(2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources;

(3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and

(4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.”

2. Statement of Interest

Since 1984, the NCS has concentrated on developing, implementing and operating the Telecommunications Services Program (TSP)¹⁸ and the Government Emergency Telecommunications Service (GETS), both National Security and Emergency Preparedness (NS/EP) priority services which provide nationwide ubiquitous voice and voice band data service in the Public Switched Telephone Network (PSTN), and, since late 2001, the Wireless Priority Service (WPS)¹⁹ which provides priority NS/EP service in the cellular wireless portion of the PSTN. All of these NS/EP priority services, authorized by the FCC as exceptions to para. 202 (a) of the Telecommunications Act of 1934, as amended, support critical functions such as national security leadership, continuity of government, U.S. population warning, public health and safety, maintenance of law and order, and disaster recovery during national security emergencies.

Current GETS and WPS services rely exclusively on the TDM circuit switched

¹⁸ See 47 C.F.R. Part 64, Appendix A [53 FR 47536, Nov. 23, 1988; 54 FR 152, Jan. 4, 1989; 54 FR 1471, Jan. 13, 1989, as amended at 67 FR 13229, Mar. 21, 2002.]

¹⁹ See Second Report and Order (FCC 00-242, WT Docket No. 96-86) The Development of Operational, Technical and Spectrum Requirements For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010 and Establishment of Rules and Requirements For Priority Access Service Adopted: July 3, 2000; Released: July 13, 2000

technology that is prevalent in the PSTN today and are implemented using a combination of national and international telephony standards and service level agreements (SLAs) with common carriers. However, DHS recognizes that the PSTN is rapidly evolving to a primarily packet-switching IP technology based infrastructure and that it is critical that today's NS/EP services evolve accordingly.

DHS believes that in the evolving IP-enabled environment both legacy voice telecommunications services and newly introduced information services must be utilized to meet NS/EP telecommunications requirements.²⁰ These NS/EP services may require government regulatory consideration to ensure the NS/EP users receive the priority treatment they need to fulfill their missions during national emergencies. NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services to Federal, state and local government officials and first responders in times of emergency or national crisis. DHS strongly encourages the FCC to include existing NS/EP considerations in the forefront of their deliberations regarding IP-enabled services.

In the Commission's recent Decision on Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges (FCC No. 04-97, WC Docket No. 02-361, adopted April 14, 2004, released April 21, 2004), AT&T's assertions that Internet protocol (IP) telephony services should be exempt from the access charges applicable to circuit-switched interexchange calls²¹ was deemed to be in error, based on interpretation of existing regulations. It is not clear to what extent the Commission's existing guidance on priority

²⁰ Report of the White House Convergence Task Force, December 29, 2000.

²¹ The *Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges* (filed Oct. 18, 2002) (*AT&T Petition*) led to the Commission's Order, FCC No. 04-97, WC Docket No. 02-361, adopted April 14, 2004, released April 21, 2004. AT&T had sought a declaratory ruling as to the applicability of interstate access charges to digital telephony services, and it asserted that such a ruling would provide guidance to

services can be either interpreted or modified to allow for NS/EP IP-enabled services requirements which are likely to evolve as technologies converge; however, the public interest would be served by considering how oversight and guidance could be provided for packet-switched NS/EP voice and data in a crisis. Any regulation of IP-based networks and IP-enabled services must preserve existing NS/EP telecommunications capabilities and allow for enhanced or evolving services as well. This regulatory challenge is made all the more complex due to the multitude of IP providers and their internetworking arrangements. Though the current NS/EP capabilities provided by the NCS are limited to voice telephony in an IP-enabled communications environment, these services will need to be expanded to meet evolving NS/EP requirements. In times of emergency or network congestion, NS/EP priority treatment may be required for certain communications such as electronic mail, instant messaging, video feeds, or video conferencing sessions. The Commission's rulemaking process must keep this in mind.

Other applications of packet-switched technology (left largely unregulated) have still been deemed to be subject to the Commission's jurisdiction; for example, the Commission recently determined that the voice over internet protocol (VoIP) service provided by pulver.com's Free World Dialup is an unregulated information service that is subject to the Commission's jurisdiction.²² In the pending rulemaking,²³ the Commission has stated: "To the extent the market for IP-enabled services is not characterized by such monopoly conditions, we seek comment on whether there is a compelling rationale for applying traditional economic regulation to providers of IP-enabled services." NS/EP considerations provide a compelling rationale for applying a certain amount of regulation to IP-enabled services. The purpose of such regulation would be to ensure the prioritized availability of certain communication services to Federal, state

(..continued)

states that mirror federal rules in assessing intrastate access charges.

²² See, footnote 10, *supra*.

²³ FCC's Proposed Rule at ¶ 5.

and local government officials and first responders in times of emergency or national crisis.

Advanced services, possibly provided via a next-generation network (NGN), are expected to become integral to NS/EP requirements. DHS has projected its broader view of NS/EP services in functional terms as follows:²⁴

1. Service Assurance - NS/EP national leadership must be assured constant availability of NS/EP user-to-user telecommunications services (wireline and wireless), without service degradation in stressed and hostile environments, with highest restoration priority in the event of loss or damage to facilities.
2. Interoperability - NS/EP national leadership must be assured seamless systems and services interoperability with current and emergent government and public services systems and networks.
3. Priority Treatment - In the event of crisis, NS/EP national leadership must receive end-to-end priority treatment over other users.
4. Ubiquitous Coverage - NS/EP national leadership must be assured seamless connectivity to government and public services and systems regardless of location.
5. Access and Identity - NS/EP national leadership must be provided the highest level of security against technological vulnerabilities. Features must include user anonymity, non-traceability, and protected access.
6. Bandwidth Services - NS/EP national leadership requires assured access to government and public telecommunications services offering integrated high quality voice, scalable data and a full-range of video services for NS/EP telecommunications.
7. Quality of Service - NS/EP traffic must be identified with its own class of service – above and beyond "best effort."

²⁴ This list is intended to be illustrative, not exclusive; other functional requirements may be identified by the NCS in

3. Statement of Position

It is the intent of DHS to take advantage of the technology developed by the industry to achieve its objectives of assured NS/EP communications during crises. The NCS intends to continue to work with the industry through voluntary and contractual arrangements, subject to Congressional budget constraints, to support NS/EP services and features. If these voluntary and contractual arrangements are insufficient to achieve assured NS/EP IP-enabled communications services, the NCS would request the FCC consider imposing regulatory constraints on all providers of IP-enabled services (e.g., LECs, IXC's, MSOs, ISPs, etc.). The regulatory agenda to be considered may need to address these needs and the Commission is respectfully requested to consider issuing guidance on these needs as part of the current Proposed Rulemaking:

1. As NS/EP priority markings are standardized by the telecommunications industry and the Government, all VoIP providers, ISPs and IP transmission carriers should not be permitted to block traffic because of the presence of an NS/EP priority marking.
2. All VoIP providers, ISPs and IP transmission carriers should not be permitted to generate NS/EP priority markings unless authorized by the Government.
3. All VoIP providers, ISPs and IP transmission carriers should transmit NS/EP markings across their networks and services, even if the respective providers do not act on the NS/EP markings.
4. All VoIP providers, ISPs and IP transmission carriers should not be permitted to provide worse service to NS/EP VoIP traffic than is provided to any non-NS/EP traffic.
5. All VoIP providers, ISPs and IP transmission carriers should be permitted to provide assured service enhancements (including priority treatment) to NS/EP marked traffic while not providing such enhancements to other traffic.
6. All VoIP providers that allow customers to communicate with users of the PSTN should be

(..continued)
the future.

required to recognize and properly route 710-NXX-XXXX calls.

B. Law Enforcement, National Security, and Public Safety

1. Background

As noted above, the United States Secret Service (“USSS”), the United States Customs Service (“USCS”), and the United States Coast Guard (“USCG”) were all transferred to DHS in the Homeland Security Act of 2002.²⁵ By the President’s Reorganization Plan of November 25, 2002, as amended by the President’s January 30, 2003 modification, the Customs enforcement functions were subsumed in the DHS Bureau of Immigration and Customs Enforcement (“ICE”).

2. Statement of Interest and Position

(a) Statement of Interest

(i) USSS

Protection of the President is paramount to the national security of the United States and represents the highest priority of the Secret Service. The ability to protect the President is a multi-faceted effort that requires robust physical and technological capabilities. Having the ability to effectively identify suspects that communicate over the internet to further their activities is critical to the successful completion of this mission. Secret Service investigative authority and capability to investigate threats represents a significant countermeasure to the ongoing war on terrorism by providing timely actionable intelligence, threat and warning information to appropriate governmental personnel. The Secret Service manages the Presidential Successor Program which is dependant, in part, on emergency communication. The Secret Service is in complete support of NCS receiving continued priority status of technologically evolving internet communication during times of national crisis. The Secret Service also

²⁵ See, footnote 6, *supra*.

investigates violations of laws relating to counterfeiting of obligations and securities of the United States; financial crimes that include, but are not limited to, access device fraud involving credit and debit cards, financial institution fraud, telecommunications and computer crimes, fraudulent identification, fraudulent government and commercial securities, electronic funds transfer fraud; and cyber-based attacks on our nation's financial, banking, and telecommunications infrastructure.

(ii) ICE

U.S. Immigration and Customs Enforcement ("ICE") is a component of the Directorate of Border and Transportation Security ("BTS") within DHS. The core functions within ICE include Immigration, Customs, and Air and Marine Enforcement, and security under the Federal Protective Service. Following is a brief description of these functions. Before turning to this description, DHS respectfully implores, *in the strongest possible terms*, that the Commission *not* reach any determinations in the context of this Proposed Rulemaking that would prejudice a determination on the CALEA Joint Petition that the intent of CALEA includes emerging technology regardless of the transmission methods and the specific type voice, electronic messaging or other technologies and services. In every operational equity discussed concerning ICE below, the ability of a malfeasor to circumvent a PEN register/court ordered wiretap through the use of IP emerging technology would substantially harm or frustrate the ICE mission and, in DHS's view, be contrary to Congressional intent for CALEA.

Air and Marine Operations

ICE's Air and Marine Operations (AMO) maintains a large fleet of aircraft and vessels strategically located through the U.S. (including Puerto Rico and the Virgin Islands). AMO's Aviation Enforcement Officers and Marine Enforcement Officers possess the skills to detect and

intercept suspect air and marine targets and to provide surveillance support to investigative entities. AMO has a number of Air and Marine Branches that conduct operations within their areas of responsibility.

Detention and Removal

Immigration Enforcement investigates violations of the criminal and administrative provisions of the Immigration and Nationality Act, as well as other provisions of the United States Code. The staff of Special Agents, Immigration Agents, and support personnel performs their duties at field offices, in task force offices, and at domestic and foreign duty posts.

The Detention and Removal program supervises and facilitates the detention and removal of aliens who are in the United States unlawfully or who are found to be deportable or inadmissible. The staff of Immigration Enforcement Agents performs their duties at field locations throughout the U.S.

Immigration Intelligence collects, analyzes, and disseminates real-time intelligence to domestic and overseas field offices. They also work with the intelligence community on intelligence matters related to national security and support integrated enforcement operations.

Federal Protective Service

The Federal Protective Service (FPS) provides security and law enforcement services to over 8,800 federally owned and leased facilities throughout the U.S. and its territories. The FPS conducts Building Security Assessments on all federally-controlled facilities to evaluate threats and tailor appropriate security countermeasures. FPS purchases, installs, and provides centralized communication, alarm monitoring, and coordination for state and federal officials regarding Federal facilities.

The FPS also coordinates over 10,000 contract security guards for federal buildings and installations across the country.

Investigations

The Investigations component of ICE enforces more than 400 different laws and regulations, including violations of law involving terrorist financing, money laundering, arms trafficking, technology exports, commercial fraud, and child pornography. ICE's investigative offices are divided geographically by areas of responsibility.²⁶

(iii) USCG

The United States Coast Guard is the nation's leading maritime homeland security agency and has broad, multi-faceted jurisdictional authority. The Operational Law Enforcement Mission is directed primarily in the areas of Boating Safety, Drug Interdiction, Living Marine Resources, Alien Migrant Interdiction and responding to vessel incidents involving violent acts or other criminal activity. The Coast Guard is additionally responsible for maritime safety, including search and rescue, aids to navigation, and distress watchkeeping. A key specific statutory authority for the USCG mission is given in 14 U.S.C. 2, "The Coast Guard shall enforce or assist in the enforcement of all applicable laws on, under and over the high seas and waters subject to the jurisdiction of the United States." In addition, 14 U.S.C. 89 provides the authority for USCG active duty commissioned, warrant and petty officers to enforce applicable U.S. law. It authorizes USCG personnel to enforce federal law on waters subject to U.S. jurisdiction and in international waters, as well as on all vessels subject to U.S. jurisdiction (including U.S., foreign and stateless

²⁶ In addition, there are a number of DHS entities that depend on the efficacy of the execution of PEN/wiretap orders in performing their infrastructure protection, law enforcement, national security and public safety missions, including the Federal Air Marshals ("FAMs"), the Transportation Security Administration ("TSA"), and the Infrastructure Protection Directorate itself.

vessels). Having the ability to effectively identify suspects that communicate over the internet to further their activities is also critical to the successful completion of this mission.

(b) Statement of Position

The Commission has stated that this proceeding will not prejudice the outcome of the forthcoming CALEA proceeding, and that the Commission will closely coordinate the IP-enabled and CALEA proceedings.²⁷ Accordingly, the Commission should not create any classifications in this proceeding that would have the effect of undermining the CALEA Joint Petition and/or CALEA's applicability to such services in general.

As noted above, DHS, by and through the USSS, USCG and ICE, engages in CALEA-related functions. These include initiating roughly 100 court ordered Title III and hundreds of "pen register" intercepts annually, as well as engaging in other investigations against terrorism in cooperation with DOJ/FBI. DHS has closely coordinated with DOJ and DHS joins with the DOJ comments on the FCC's Proposed Rule that the Commission should adopt non-economic regulations to ensure that current and emerging IP-Enabled Services, including VoIP, do not endanger critical law enforcement, national security, and public safety policies of the Executive Branch. In order to maintain the capability to provide effective investigative protection to the President of the United States (POTUS) and other designees covered by DHS interests, and the support to law enforcement and infrastructure protection missions DHS serves, we concur with DOJ and urge the Commission in the strongest possible terms that CALEA should apply to all of the IP-Enabled Services discussed in the CALEA Joint Petition.

²⁷ Proposed Rule at ¶ 50 n. 158.

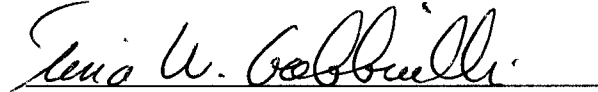
IV. Conclusion

DHS welcomes the opportunity to contribute to this important initiative. DHS appreciates the Commission's recognition that ability to protect the Nation's critical infrastructure protection, law enforcement, national security, and public safety needs entrusted to the Executive Branch must be maintained in deciding the course of the Commission's treatment of emerging IP-Enabled Services. In close coordination with the Department of Justice, the Department of Homeland Security strongly maintains that the public interest would be served by integrating the foregoing needs for both the telecommunications and the information technology infrastructures into the Commission's IP-Enabled Services regulatory strategy for the United States, and we share the DOJ's law enforcement and national security concerns regarding access to sensitive network information and authorizations to provide international communications services.

Respectfully submitted,

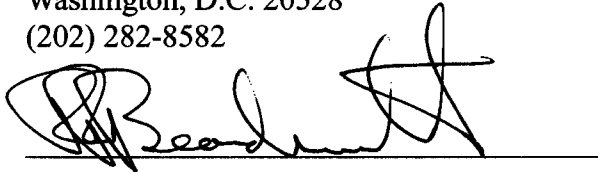
**UNITED STATES DEPARTMENT OF
HOMELAND SECURITY**

By:



Tina W. Gabbrielli
Director of Intelligence Coordination and
Special Infrastructure Protection Programs
Information Analysis and Infrastructure
Protection Directorate
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8582

By:



Randy Beardsworth
Director of Operations
Border and Transportation Security Directorate
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
Nebraska Avenue Complex
Washington, D.C. 20528
(202) 282-8028

Date: May 28, 2004